

**UNITED STATES DISTRICT COURT  
DISTRICT OF MAINE**

IN THE MATTER OF THE SEARCH	)	
OF INFORMATION ASSOCIATED	)	Docket No. <u>2:22-mj-164-KFW</u>
WITH FACEBOOK USER ID 50260419 /	)	
USERNAME: RON.BUSH.9 AND	)	
USER ID 100000588099672 /	)	
USERNAME:STEPHANIE.POLLOCK.395	)	
STORED AT PREMISES CONTROLLED BY	)	
META PLATFORMS, INC.	)	

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Anthony Castellanos, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent (SA) with HSI and have been since 2007. During my tenure with HSI, I have investigated numerous federal criminal violations related to cybercrime, child exploitation and child pornography. In my career, I have used various investigative tools and techniques including search warrants for electronic information in the possession of electronic service providers (ESP) and electronic devices. Since 2016, I was certified as a Computer Forensics Agent (CFA) by the HSI Cyber Crimes Center (C3). I am certified to conduct forensic analysis on computers, cell phones, and other digital devices and media. I have not included every detail of every aspect of my training, education, and experience but have highlighted those areas most relevant to this application. The facts in this affidavit come from my personal observations, my training and experience and information obtained from other agents, law enforcement officers and witnesses.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe a violation of Title 18, United States Code, Section § 2251(a), production of child pornography; 18 U.S.C. §§ 2252A(a)(5)(B) and 2252(a)(4)(B), possession of

child pornography; and 18 U.S.C. §§ 2252A(a)(2) and 2252(a)(2), distribution and receipt of child pornography was committed by Bianca VANVALKENBURG, Ron A. BUSH and others. There is also probable cause to search the locations described in Attachment A for evidence of these crimes, as described in Attachment B.

3. I make this affidavit in support of an application for a search warrant for content and records associated with the Facebook accounts assigned user IDs 502604195 and 100000588099672, which are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., an electronic service provider located in Menlo Park, California. The information and account to be searched are described herein and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta Platforms, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account referenced in this affidavit and further in Attachment A, including the contents of the communications.

4. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that - has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

5. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Meta Platforms, Inc. to disclose to the government copies of the records and other

information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### **STATUTORY AUTHORITY**

6. Title 18, United States Code, Section 2252(a)(2) prohibits the knowing receipt or distribution of any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in or affecting interstate or foreign commerce, by any means, including by computer.

7. Title 18, United States Code, Section 2252A(a)(5)(B) prohibits the knowing possession of any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

8. Title 18, United States Code, Section 2422(b) prohibits any person from using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or to attempt to do so.

9. Title 18, United States Code, Section 2256(1) defines “minor” as any person under the age of eighteen years.

10. Title 18, United States Code, Section 2256(8) defines “Child Pornography” as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct; or, (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.”

11. Title 18, United States Code, Section 2256(2) defines “sexually explicit conduct” as actual or simulated: (i) Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) Bestiality; (iii) Masturbation; (iv) Sadistic or masochistic abuse; or (v) Lascivious exhibition of the anus, genitals, or pubic area of any person.

12. Title 18, United States Code, Section 2256(5) defines “visual depiction” as including undeveloped film and videotape, and data stored on computer disk or by electronic means that is capable of conversion into a visual image.

#### **TECHNICAL INFORMATION REGARDING FACEBOOK**

13. Meta Platforms, Inc. formerly Facebook, Inc., owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

14. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

15. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

16. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

17. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items

available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

18. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

19. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

20. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

21. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

22. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

23. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

24. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

25. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

26. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a

Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

27. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

28. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access



their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Therefore, the computers of Meta Platforms, Inc. are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

#### **PROBABLE CAUSE**

30. On March 30, 2020, the National Center for Missing & Exploited Children (NCMEC) received a cyber tip (#66879510) from Facebook, Inc. The cyber tip indicated that on or about March 28, 2020, the Facebook user ID 502604195 (username: ron.bush.9), registered to Ron A. BUSH, uploaded at least one suspected child pornography file to Facebook Messenger. Approximately eight minutes before the file upload, Facebook, Inc. recorded BUSH’s IP address

as 2603:9000:1f13:5f3b:3846:ed12:5b90:1d5d. Additionally, the cyber tip indicated Facebook user ID 100000588099672 (username: stephanie.pollock.395), registered to Stephanie Pollock, was the recipient of the suspect file.

31. On April 21, 2020, the Hillsborough County Sheriff's Office (HCSO) received NCMEC cyber tip #66879510. Pursuant to a subpoena, HCSO learned IP address 2603:9000:1f13:5f3b:3846:ed12:5b90:1d5d was registered to Kim Young at 1019 Leisure Ave, Tampa, Florida 33613.

32. On August 22, 2020, at approximately 0816 hours, two HCSO detectives arrived at 1019 Leisure Ave, Tampa, Florida 33613. Detectives audio recorded their encounter with the residents. An unidentified female can be heard yelling for "Red" when detectives asked to speak with Ron BUSH. An unidentified male, later identified as BUSH, agreed to talk to the detectives. In sum and in substance, the following was learned from BUSH during the noncustodial interview with HCSO detectives:

- a. BUSH's primary cell phone was an Android phone, later identified as an LG phone. He had owned the LG phone for approximately two years. The LG phone was used by BUSH to access his Facebook account.
- b. BUSH's Facebook account was shut down approximately a year ago for unknown reasons.
- c. BUSH confirmed his date of birth (10-08-1981) and two email addresses (xargonbr@gmail.com & hudsonhawkbr1@gmail.com). The date of birth email addresses were associated with his Facebook account and were detailed in the NCMEC cyber tip #66879510.

- d. BUSH admitted to forwarding images to Stephanie Pollock via Facebook. BUSH stated the images were of a rash on his friend's son's "ball sack." BUSH also indicated there was a folder on his phone containing the files he received from his friend which he subsequently forwarded to Pollock. BUSH deleted the folder several times, including moments before he handed his LG phone to HCSO detectives. BUSH suspected the files kept reappearing because of Dropbox. BUSH downloaded Dropbox approximately four years ago with his email hudsonhawkbr1@gmail.com. BUSH added he was not a regular user of the Dropbox application.
- e. BUSH also confirmed sending the image provided in the NCMEC cyber tip #66879510 when shown the image.

33. As of result of the interview, HCSO detectives detained BUSH's LG phone pending a search warrant. On September 23, 2020, the LG phone was transferred to the Tampa Police Department (TPD) for forensic data extraction pursuant to a search warrant.

34. On September 23, 2020, BUSH left a voicemail to one of the HCSO detective. In the voicemail, BUSH confirmed the existence of a folder labeled, "MINOR"<sup>1</sup> which contained the images his friend had sent of her son. BUSH also said he had downloaded other items to the "MINOR" folder.

35. On September 28, 2020, a TPD examiner conducted an advance logical extraction of BUSH's LG phone. Additionally, the TPD examiner imaged a 32GB MicroSD card associated

---

<sup>1</sup> The name of the folder is the minor's actual birth given name. For the purpose of this affidavit and the protection of the child, all references to the folder and the child will be referred to as "MINOR."

with the LG phone. On September 30, 2020, the extracted data and the LG phone were provided back to HCSO.

36. On October 5, 2020, at approximately 1228 hours, BUSH met with HCSO detectives to discuss the “MINOR” folder and other findings recovered from his LG phone. In sum and in substance the following was learned from BUSH:

- a. BUSH identified Bianca VANVALKENBURG as the sender of the suspect files found in the “MINOR” folder. BUSH also provided HCSO with one of VANVALKENBURG’s social media accounts.
- b. BUSH met VANVALKENBURG via her DOM<sup>2</sup> -- an unidentified male. Later, BUSH and VANVALKENBURG did a sex scene at a local hotel.
- c. BUSH stated VANVALKENBURG was originally from Florida and moved “north” perhaps due to an outstanding warrant, but he was unsure. VANVALKENBURG moved approximately two or three weeks after they met for their sex scene.
- d. BUSH explained VANVALKENBURG had a child in Florida who was given up for adoption. Once VANVALKENBURG moved north, she had her second child, whom BUSH identified as MINOR.
- e. BUSH and VANVALKENBURG only communicated via the Kik application. BUSH saved everything sent by VANVALKENBURG into the “MINOR” folder.

---

<sup>2</sup> The dominant person in a BDSM relationship or encounter.

- f. BUSH explained he was having a conversation with VANVALKENBURG about MINOR's diaper rash when VANVALKENBURG sent the files. BUSH agreed to forward the files to Pollock since Pollock worked in the nursing field.
- g. BUSH admitted to opening one of the videos which depicted VANVALKENBURG "working" <sup>3</sup> him [MINOR].
- h. BUSH suspected VANVALKENBURG felt comfortable sending him those files since he had reputation in the BDSM<sup>4</sup> community as a DOM who respected people's kinks.
- i. BUSH confirmed he no longer had the Kik application installed on his phone.

37. On October 5, 2020, HCSO contacted the Maine State Police (MSP) Computer Crimes Unit (CCU) and informed them about their findings concerning Bianca VANVALKENBURG. HCSO also provided CCU with two of the videos recovered from BUSH's phone.

38. On October 6, 2020, MSP SA Glenn Lang conducted record checks and learned Bianca VANVALKENBURG, with date of birth September 2, 1994, had a listed address of 12 Knox St. Apt 2, Rockland, Maine. SA Lang spoke with DHHS and learned MINOR was seized from VANVALKENBURG in March of 2019. Additionally, DHHS seized VANVALKENBURG's third child in February of 2020 upon the child's birth.

39. On October 7, 2020, SA Lang reviewed the videos sent by HCSO. SA Lang could hear a dispatch center and possibly fire trucks returning to their station. SA Lang used software

---

<sup>3</sup> HCSO Detective confirmed BUSH's statement to mean VANVALKENBURG was masturbating the MINOR.

<sup>4</sup> BDSM initialism - Bondage & Discipline Domination & Submission, Sadism & Masochism.

to separate the audio from the video. The audio was sent to the Rockland Dispatch Center (RDC) for review. A RDC supervisor confirmed the voice of one of the dispatchers heard in the audio.

40. On October 21, 2020, MSP obtained a state warrant for VANVALKENBURG's residence located at 12 Knox St. Apt 2, Rockland, Maine. That same day, at approximately 1543 hours, MSP and the Rockland Police Department (RPD), executed the state search warrant.

41. During the warrant, MSP SA Lang and RPD Detective Alex Gaylor interviewed VANVALKENBURG. In sum and in substance, VANVALKENBURG stated the following:

- a. VANVALKENBURG was not familiar with the name Ron BUSH.
- b. VANVALKENBURG grew up in Florida and had friends there.
- c. VANVALKENBURG utilized Facebook Messenger, Instagram, Twitter but had not used Kik since she got her new phone in January of 2020.
- d. VANVALKENBURG confirmed the presence of a police scanner at her mother's residence, later determined to be Apt #7 of the same complex.
- e. When presented the evidence recovered from BUSH's phone, VANVALKENBURG stated a person, later identified only as "Red" twisted her arm and blackmailed her in sending the files. VANVALKENBURG met "Red" via a mutual friend only identified as "RICO." VANVALKENBURG described "Red" as a white bulker guy in his thirties with red hair.
- f. VANVALKENBURG confirmed filming a sex video with "Red" in a hotel room. During this time, VANVALKENBURG was staying in Florida with "RICO."
- g. VANVALKENBURG explained "Red" told her that if she did not send the files he wanted, he was going to provide her mother's name to a person(s) known to have killed people. VANVALKENBURG took this as a threat to have her mother

killed. VANVALKENBURG explained all the threats were made via the calling feature on the Kik application.

- h. “Red” requested pictures and videos of MINOR’s privates. At least one of the requests was of her jerking MINOR off. VANVALKENBURG confirmed the video was made at her mother’s residence, specifically, the living room. The video was filmed with her iPhone 5 SE. VANVALKENBURG volunteered to provide law enforcement the iPhone 5 SE.
- i. VANVALKENBURG stated she deleted the files after sending them. VANVALKENBURG claimed no other electronic device of hers contained those related media files.
- j. When shown a screenshot of the video, VANVALKENBURG confirmed it was her hand in the video. VANVALKENBURG later confirmed she used her right hand to masturbate MINOR.
- k. VANVALKENBURG suspected the files were created after June of 2018 (MINOR’s birth) and before November of 2018, when she moved into her current apartment. However, VANVALKENBURG was unsure of the exact date and time.
- l. VANVALKENBURG speculated she sent approximately twenty images and/or videos of MINOR to “Red.” VANVALKENBURG also stated “Red” requested videos of her sucking and licking MINOR’s penis, but she initially did not recall doing those acts on MINOR. VANVALKENBURG did not recall since she was under stress and PTSD, coupled with “Red’s” threats. VANVALKENBURG did remember sending a picture of her kissing the tip of MINOR’s penis.

VANVALKENBURG later admitted to sucking, kissing, licking and jerking MINOR's penis.

- m. "Red" also requested VANVALKENBURG sit on MINOR's penis after getting it hard, but VANVALKENBURG refused. VANVALKENBURG also refused to do anything involving MINOR's anus because she knew that was traumatic.

VANVALKENBURG stated she only did things she was comfortable doing given "Red's" threats. VANVALKENBURG also felt reassured when "Red" explained MINOR was too young to remember anyways.

- n. The last time VANVALKENBURG had contact with "Red" was when she attempted to contact "Red" in March of 2019. VANVALKENBURG indicated this was after she had sent the files of MINOR. VANVALKENBURG reached out because Florida had been hit with a bad storm and she wanted to confirm how "Red" was doing. VANVALKENBURG later stated she was more interested in finding out how "Red's" roommate and roommate's child were doing.
- o. VANVALKENBURG never reported the threats to anyone because she previously reported her grandfather and uncle molesting her for over 10 years and no one believed her.
- p. VANVALKENBURG also admitted to sending the images and videos to "RICO" after he threatened her. VANVALKENBURG explained "RICO" was prior military and had legally killed people in a war. VANVALKENBURG felt "RICO" was more of a threat than "Red." VANVALKENBURG also clarified it was "RICO" that "Red" was going to contact when "Red" threatened to provide her mother's name to people who have killed.



q. VANVALKENBURG stated she had PTSD, depression, anxiety and chronic pain due to a degenerative disease.

42. As a result of the MSP search warrant, four cellular phones and one laptop were seized from VANVALKENBURG's residence.

43. On October 22, 2020, officials with the Maine Department of Health & Human Services (DHHS) met with VANVALKENBURG for another interview. VANVALKENBURG reiterated many the of statements she made SA Lang and Det Gaylor. However, during this interview, VANVALKENBURG introduced "Red" as friend she had while she resided in Florida. Additionally, VANVALKENBURG stated "RICO" was a sniper in the Army and he now lived in New Hampshire.

44. On April 23, 2021, MSP completed their forensic analysis of the seized electronic devices. The analysis revealed no child exploitation material on VANVALKENBURG's devices and no Facebook Messenger content was recovered.

45. In December 2021, I was able to review evidence recovered from BUSH's LG phone. I only observed an advance logical extraction conducted on the LG phone. As a result of this extraction method, many third-party application datasets were potentially not recovered. However, I was able to observe the media files recovered from the "MINOR" folder.

46. In total, there were twenty-five (25) media files recovered from the "MINOR" folder. Eleven (11) images and four (4) videos were associated with MINOR. The eleven (11) images depicted and focused on MINOR's genital area; none revealed the MINOR's face. Some images depict a hand holding/touching MINOR's penis. Additionally, one image depicted VANVALKENBURG's face in the background while MINOR's penis was the primary focus. The four (4) videos were each 15 seconds in duration and depicted MINOR getting masturbated.

47. On January 10, 2022, a HSI Special Agent from the Tampa Field Office was able to take custody of BUSH's LG phone after coordinating with the HCSO. The LG phone was overnighted to the HSI Portland, Maine Field Office for further examination.

48. On January 11, 2022, I received a FedEx package containing BUSH's LG phone and it was secured in the forensic lab.

49. On January 13, 2022, this Court issued a search warrant authorizing a renewed search of BUSH's LG phone. A full filesystem extraction was successfully conducted on BUSH's LG phone. A review of the data did not reveal additional evidence as it relates to this investigation. Additionally, no Facebook Messenger content was recovered.

50. Based on the above, I believe that child sexual abuse material was transmitted from the Facebook user ID 502604195 (username: ron.bush.9) to the Facebook user ID 100000588099672 (username: stephanie.pollock.395) between June of 2018 and March of 2020.<sup>5</sup> I further believe that the child sexual abuse material at issue was created in the District of Maine and initially transmitted to Ron BUSH from the District of Maine. I therefore believe fruits, instrumentalities, and evidence of the above-stated crimes will be found in Facebook user ID 502604195 (username: ron.bush.9) and Facebook user ID 100000588099672 (username: stephanie.pollock.395) and the linked Facebook Messenger application.

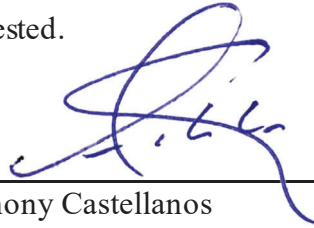
### **CONCLUSION**

51. Based on my training and experience, and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that the Facebook accounts described

---

<sup>5</sup> Although the child sexual abuse material (CSAM) involved in the NCMEC referral may not be a child from Maine, I believe the March 2020 sharing of CSAM between BUSH and POLLOCK is evidence of an ongoing CSAM sharing relationship. This is evidence of intent as it relates to the reasons for sharing the contents of the MINOR folder as described above.

in Attachment A contains the fruits, instrumentalities, and evidence of crimes described in Attachment B. Accordingly, a search warrant is requested.

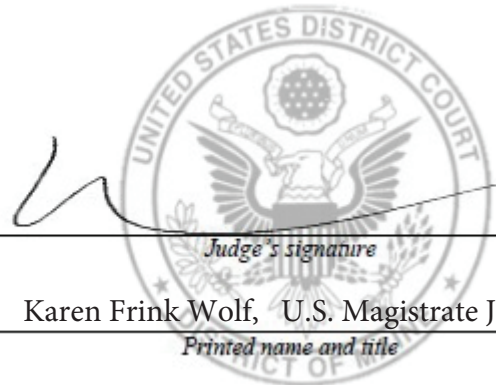


Anthony Castellanos  
Special Agent  
Homeland Security Investigations

Sworn to telephonically and signed  
electronically in accordance with the  
requirements of Rule 4.1 of the Federal Rules  
of Criminal Procedures

Date: Sep 23 2022

City and state: Portland, Maine



*Judge's signature*

Karen Frink Wolf, U.S. Magistrate Judge

*Printed name and title*